I. Introduction

Most of the conventional erasure-correcting codes show a distance-bounded characteristic [1]. In other words, the conventional codes can recover erased data within their capability. The capability is related to the code rate. According to the Singleton bound [1], [2], fewer than \( n-k \) erasures can be corrected by the \((n, k)\) erasure-correcting code whose code rate is \( k/n \). The codeword length is \( n \), and the number of message symbols is \( k \). Thus, erasure-correcting capability is increased if the code rate is decreased. However, the channel goodput is reduced if more redundant symbols than the number of erasures are transmitted. Thus, an accurate estimation of the erasure rate is required to increase the goodput. However, the code rate of the conventional erasure-correcting code is determined by the transmitter. Thus, in addition, a feedback channel to inform erasure rate is required.

The rateless code is a new class of erasure-correcting code. The encoding procedure of a rateless code is repeated until the whole message is recovered perfectly at the receiver [3]. Thus, the rate of a rateless code is determined by the receiver. Hence, the goodput is increased if the number of redundant symbols is minimized. Also, the additional process and the feedback channel related with erasure rate are not required. Thus, research about rateless codes has been gaining popularity over the last decade [3]-[13].

The Luby transform (LT) [3] code is the first generation of rateless codes. The LT encoding scheme, in which message symbols are selected as many times as the generated degrees, is used in rateless codes [3], [4]. In addition, the belief propagation (BP) decoding scheme [3], [4] is used because of the low computational complexity [3]. However, the LT code requires more redundant symbols than expected to recover all messages.
the messages [5].

Whereas a uniform selection of messages in the encoding procedure is usually used for equal error protection (EEP), nonuniform selection is used for unequal error protection (UEP). However, a rateless code using nonuniform selection requires fewer redundant symbols than one using a uniform selection scheme, not only in UEP but also in EEP [6], [7]. The encoding scheme using nonuniform selection in the former results was also designed for UEP. Hence, the messages were classified into several groups according to their priorities. In addition, selection probabilities according to the classified groups were given in advance. In the previous research [6], [7], messages were classified for convenience into two groups: the more important block (MIB) and the less important block (LIB). According to the simulation results, the MIB clearly performs better than the LIB. However, even the LIB performs better than the case of EEP with small redundant symbols in terms of error rate because the probability of recovering a message with fewer codewords is increased by the nonuniform selection of messages. Thus, the rateless code with the nonuniform selection scheme for UEP shows better error performance than the rateless code with uniform selection for EEP. However, there is no research on the application of the nonuniform selection scheme to rateless codes for EEP.

Accordingly, a scheme to classify messages for EEP and an encoding scheme using nonuniform selection were proposed in our previous work [8], and fewer redundant symbols were required by the proposed encoding scheme. However, a certain number of degrees should be generated to classify messages in advance [8]. Thus, a new encoding scheme using nonuniform selection without the pre-generation of degrees is proposed and analyzed in this paper. In addition, a new hybrid decoding scheme to make up for the drawbacks of the BP decoding scheme is proposed and analyzed.

II. Uniform Selection Encoding and BP Decoding

The LT code with uniform selection of messages generates limitless codewords until the full messages are recovered at the receiver. The encoding process is as follows.

At first, degree $d$, which is the number of messages added to a codeword symbol, is chosen at random according to a degree distribution $\rho(d)$. Among $k$ messages, $d$ distinct message symbols are selected uniformly. Then, the selected $d$ message symbols are bit-wisely summed. The BP decoding scheme is started with the searching of a degree-1 codeword. A codeword with degree-1 is relevant to a message because the probability is increased as the slope is decreased since the recovered messages are selected with the same probability as the unrecovered messages. Consequently, the probability to recover a message is decreased since the recovered messages are selected with the same probability as the unrecovered messages.

This phenomenon is shown in Fig. 1. The figure represents the average number of recovered messages according to the number of received codewords at $k=500$ and a binary erasure channel (BEC) with an erasure rate $e=0.1$. The slope of the graph can be regarded as the probability of recovering a message because the probability is increased as the slope is increased. According to the results, the slope of the BP algorithm is almost 0 if the number of recovered messages is smaller than about 50. Further, only 11 messages are recovered from 500 codewords.

In contrast, the slope of the maximum likelihood (ML) algorithm is constant. The encoding procedure can be represented as $\mathbf{U}=\mathbf{G}\mathbf{m}$. The codeword and message vector are $\mathbf{U}$ and $\mathbf{m}$, respectively, and the generating matrix is $\mathbf{G}$. The decoding process is equal to solve the equation. Thus, any
message would be recovered by the ML algorithm if \( \mathbf{G} \) were invertible \([4]\). In other words, a new message can be recovered by the ML algorithm if a received codeword is connected to an unrecovered message. However the BP decoding cannot be done if there is no degree-\( d \) codeword connected with the \( d-1 \) recovered message. As a result, it is difficult to recover a new message connected to codewords with a uniform probability using the BP decoding algorithm.

### III. Proposed Encoding and Decoding Schemes

#### 1. Proposed Encoding Scheme

Messages can be recovered with different probabilities according to the degrees of the connected codewords. A new message symbol can be recovered from the received degree-1 codeword. Hence, a message symbol that is connected to the degree-1 codeword can be recovered with the highest probability of \( (1-\varepsilon) \) at the BEC. Here, \( \varepsilon \) is the erasure rate, as mentioned in section II. A new message symbol should be recovered from a codeword with any other degree to conduct the BP decoding procedure successively. Therefore, \( d-1 \) recovered messages and an unrecovered message should be added to a degree-\( d \) codeword. However, the probability that \( d-1 \) messages will be recovered from a degree-\( d \) codeword at the BEC is \( (1-\varepsilon)^{d-1} \) at most when the codewords meet the upper condition. Therefore, the probability to recover a new message symbol is increased if the degree of a codeword is decreased. Only one message should be connected to the recovered message if the degree of the codeword is 2 among any other degrees. Therefore, a message is recovered from the degree-2 codeword symbols with the second highest probability of \( (1-\varepsilon)^2 \).

Accordingly, the total messages \( \mathbf{M} \) are classified into two sets, \( \mathbf{M_1} \) and \( \mathbf{M_2} \). The whole set \( \mathbf{M} \) is \( \mathbf{M_1}+\mathbf{M_2} \), (that is, \( \mathbf{M_1} \cap \mathbf{M_2} = \emptyset \) and \( \mathbf{M_1} \cup \mathbf{M_2} = \mathbf{M} \)). Sets \( \mathbf{M_1} \) and \( \mathbf{M_2} \) are the sets whose messages are connected to degree-1 and degree-2 codewords, respectively. Hence, messages in \( \mathbf{M_1} \) are recovered with the highest probability, and the ones in \( \mathbf{M_2} \) are recovered with the second highest probability. Therefore, when choosing two messages with a ratio of \( R_{TH} \) from among degree-2 codewords, if one message is selected from \( \mathbf{M_1} \), which is a neighbor of the degree-1 codeword, and the other from \( \mathbf{M_2} \), new messages can be recovered from degree-2 codewords with higher probability. Here, \( R_{TH} \) is the probability that a message in \( \mathbf{M_1} \) is selected.

At first, \( \mathbf{M_1} \) is determined in the proposed encoding scheme, as shown in Fig. 2. The easiest way to find \( \mathbf{M_1} \) is searching degree-1 codewords directly from a sufficient number of codewords for the perfect recovery of messages. Hence, we call this a direct search (DS) scheme. However there is no need to generate every codeword and check the messages connected to the codewords because messages are selected at random in the encoding procedure. Thus, \( \mathbf{M_1} \) can be randomly chosen as many times as \( N_1 \) from \( \mathbf{M} \), \( N_1 \) being the number of degree-1 codewords in a sufficient number of codewords. The DS method was proposed in our previous work \([8]\). Searching \( N_1 \) from a certain number of codewords is approximated by

\[
N_1 \equiv \rho(1) \cdot n, \tag{2}
\]

where \( \rho(1) \) is the degree distribution for degree-1 and \( n \) is the number of codeword symbols required for perfect recovery. However, a certain number of degrees should be generated to find \( N_1 \) in advance. Another alternative is the replacement of \( N_1 \) with its probabilistic expectation. The probability that a codeword has the degree \( d \) at each generation is \( \rho(d) \). Hence, there can be \( \rho(1)n \) degree-1 codewords if \( n \) codewords are generated and each generation of degree is independent. Therefore, there can be as many degree-1 codewords as the expectation of \( N_1 \) with the highest probability because the expectation is the value with the highest probability of occurrence. Thus, we call this a probabilistic expectation (PE) scheme. The PE of \( N_1 \) is represented by

\[
E(N_1) \equiv \rho(1) \cdot E(n). \tag{3}
\]

Then, a message symbol is chosen from the different sets \( \mathbf{M_1} \), \( \mathbf{M_2} \), and \( \mathbf{M} \) according to the degree \( d_j \) of the \( j \)-th codeword symbol. A message is selected from \( \mathbf{M_1} \) if the \( d_j \) is 1. If the \( d_j \) is 2 and \( n_r \) is smaller than \( R_{TH} \), one message is chosen from \( \mathbf{M_1} \) and the other is chosen from \( \mathbf{M_2} \). A randomly generated number in \((0, 1)\) is represented by \( n_r \). On the contrary, messages are selected uniformly if \( d_j \) is more than 2 or \( n_r \) is bigger than \( R_{TH} \) even though \( d_j \) is 2. Thus, the proposed encoding scheme
Fig. 2. Proposed scheme of nonuniform selection of messages in encoding.

Fig. 3. Proposed BP-GE hybrid decoding scheme.

is equal to the conventional encoding scheme if $R_{TH}$ is 0. This encoding procedure is repeated until every message is recovered like in the conventional encoding scheme with a uniform selection of messages.

2. Proposed Decoding Scheme

The BP or ML algorithm is generally used as a decoding scheme for rateless codes. With the probability $1 - \delta$ by the BP algorithm, $k$ messages can be recovered from any $k + O(\sqrt{k \ln^2 (k / \delta))}$ of codewords [9]. In other words, $O(\sqrt{k \ln^2 (k / \delta))}$ more codewords are required. However, $O(\log_2 (1 / \delta))$ more codewords are required if ML is used as a decoding scheme [7]. Thus, ML requires less overhead than BP. In contrast, the BP scheme and the ML scheme need $O(k \ln(k / \delta))$ and $O(k^2)$ symbol operations, respectively [9]. Hence, the ML scheme has more computational complexity if the same number of message symbols should be recovered. Thus, BP and ML have different merits and demerits. However, the computational complexity of ML is decreased relatively more than BP if the number of messages to be recovered is decreased, because the computational complexity of the ML algorithm is entirely dependent on the number of messages. In the case of the BEC, ML decoding is equal to the Gaussian elimination (GE) [4]. Thus, the BP-GE hybrid decoding scheme is proposed in this paper. At first, BP decoding is used until more than an $R_{HB}$ portion of messages is recovered, as shown in Fig. 3. Here, $i$ is the number of recovered messages. After BP decoding, GE decoding is applied.

IV. Performance Comparison and Analysis

The performances of the proposed encoding and decoding schemes are compared with the performances of the conventional schemes and analyzed in our simulation. The performances are compared in terms of goodput and computational complexity. Goodput is the ratio of the successfully received amount of message symbols to the total transmission time [14]. Thus, goodput $\gamma$ can be defined as

$$\gamma = \frac{m}{t} = \frac{m}{d} \cdot \frac{d}{t},$$

(4)

where $m$ is the number of successfully received messages and $t$ is the transmission time. In addition, $d$ is the total number of transmitted data. Thus, a $d/t$ ratio is a data rate, which is determined by the communication system. Hence, goodput can be represented simply as $m/d$ if we exclude the effect of the specific communication system.

Transmitted data includes message and overhead. Overhead consists of various protocol headers and redundant symbols. However, the amount of a protocol header is fixed according to the various applications, and it is quite smaller than that of redundant symbols. Thus, the goodput can be approximated to a ratio between the amount of messages and overhead except for the protocol headers. In addition, in the case of a rateless
code, redundant symbols are generated limitlessly until all the messages are recovered successfully at the receiver. Thus, the numerator of goodput is fixed to the number of message symbols, and the denominator varies according to the amount of overhead. Therefore, the amount of overhead is inversely proportional to goodput. Hence, the average amount of overhead can be used as a simple performance measure of goodput. Accordingly, the average overhead and the number of symbol operations are used as performance measures in this paper.

The appropriate $R_{TH}$ and $R_{HB}$ for the proposed encoding and decoding schemes are searched experimentally. To find the best $R_{TH}$ and $R_{HB}$, $R_{TH}$ is increased from 0.0 to 1.0 and $R_{HB}$ is decreased from 1.0 to 0.1. In our simulation, robust soliton degree distribution [3], which is a well-known degree distribution for the uniform selection scheme, is adopted regardless of the encoding scheme to compare the performance of uniform and nonuniform selection. The maximum number of transmitted codewords is set to 10 times that of the message size. We use $10^6$ message frames with the size of 500 symbols and 5,000 symbols. Results in a BEC environment with an erasure rate from 0% to 20% are presented.

1. Performance According to Encoding Schemes

Figure 4 shows the average overhead according to the message selection scheme and $R_{TH}$ for nonuniform selection at $k=500$. Here, $R_{TH}=0.0$ corresponds to the conventional uniform selection scheme. First, $N_1$ is determined by the DS scheme in the case of nonuniform selection. According to Fig. 4, the uniform selection encoding scheme requires a 31.1% average overhead at a 10% erasure rate. The proposed encoding scheme using nonuniform selection needs 24.6%, 23.3%, 24.7%, and 26.4% at $R_{TH}=0.05$, 0.1, 0.2, and 0.3, respectively. Therefore, the nonuniform encoding scheme, in which $N_1$ is searched by the DS scheme, has approximately 6.5%, 7.8%, 6.4%, and 4.7% less overhead than the conventional encoding scheme using uniform selection. Average overhead at an erasure rate of 10% according to the various $R_{TH}$ for nonuniform selection is shown in Fig. 5. According to the results, the minimum overhead is obtained at about $R_{TH}=0.1$. The degree-2 codewords are connected more frequently to the already recovered messages as $R_{TH}$ is increased more than 0.1. Thus, the probability of recovering a new message is also considered to be decreased if $R_{TH}$ is decreased less than 0.1. There is little variation in the relationship between both encoding schemes as the erasure rate varies.

According to Fig. 6, the effect of nonuniform selection is apparent. Figure 6 shows the average number of recovered messages according to the number of received codewords at $k=500$ and $ε=0.1$. When the number of received messages is fewer than about 600, the number of recovered messages is increased as $R_{TH}$ is increased because messages connected to degree-2 codewords are connected to degree-1 codewords more frequently as $R_{TH}$ is increased. Thus, the probability of recovering a new message from degree-2 codewords is also increased. On the contrary, when more than approximately 600 codewords are received or 300 messages are recovered, the number of recovered messages is relatively decreased as $R_{TH}$ is increased. In addition, the number of recovered messages is also decreased regardless of the number of received codewords as $R_{TH}$ is decreased less than 0.1. In this case, it is considered that the effect of the nonuniform selection cannot be obtained.
Thus, the effect of the nonuniform selection is considered to be maximized at $R_{TH}=0.1$.

Figure 7 shows the average overhead according to the algorithms for the determination of $N_1$ at $k=500$ and $R_{TH}=0.1$. The PE can replace $N_1$. There can be 3.9 degree-1 codewords among 500 codewords because $\rho(1)=7.81 \times 10^{-3}$. Thus, $N_1=3$, 4, and 5 are considered around the expectation. In addition, the BP decoding scheme is used in common. According to the simulation results, 23.9%, 23.6%, and 23.5% overhead is required at $N_1=3$, 4, and 5, respectively, when $\epsilon=0.1$. Thus, there is little difference in average overhead according to the variation of $N_1$, although $N_1=5$ requires the least overhead.

Further, almost the same overhead is required by the PE scheme as is required by the DS scheme. Thus, $N_1$ can be replaced with the PE.

Figure 8 shows the average overhead according to the encoding schemes at $k=5,000$. There can be about 13.7 degree-1 codewords among 5,000 codewords because $\rho(1)=2.74 \times 10^{-3}$. Thus, $N_1=13$, 14, and 15 can be considered in the case of the PE scheme. When the PE scheme is used, $N_1$ is set to 15 among them. Less overhead than uniform encoding is required by the proposed nonuniform encoding scheme, although the message size is increased from 500 to 5,000. Uniform encoding requires a 17.9% average overhead at a 10% erasure rate. However, the nonuniform encoding scheme by the DS method requires 16.4% and 16.9% overhead at $R_{TH}=0.1$ and 0.2, respectively. Hence, 1.5% and 1% less overhead is required by the nonuniform encoding scheme. In addition, the nonuniform encoding scheme with the PE or DS algorithm requires almost the same overhead. However, the difference between the uniform and nonuniform encoding schemes is decreased as the message size is increased. According to [15], the LT code requires less overhead as the messages increase. Thus, the reduction of improvement is caused by the increase in the message size.

The average number of symbol operations is shown in Tables 1 and 2. The proposed encoding scheme at $k=500$ and $N_1=5$ requires 9.3, 9.46, and 9.61 symbol operations per message at $R_{TH}=0.1$, 0.2, and 0.3, respectively, as shown in Table 1. However, the encoding scheme using uniform selection needs 10.7. Thus, the proposed encoding scheme with less overhead also requires fewer symbol operations because
nearly all the edges connected to the received codewords are removed with the BP decoding procedure. In addition, the proposed encoding scheme also requires fewer symbol operations, although the message size is increased from 500 to 5,000, as shown in Table 2. Therefore, less overhead and a fewer number of symbol operations are required by the proposed nonuniform encoding scheme as compared to the conventional uniform encoding scheme.

2. Performance According to Decoding Schemes

Average overhead according to decoding schemes is represented in Fig. 9. The nonuniform selection scheme with the PE algorithm is used as an encoding scheme in each case. In this simulation, $N_1$ is set to 5. The GE requires less overhead than the BP if the number of messages to be recovered is the same. For example, the BP-GE hybrid decoding at a 10% erasure rate requires 21.1%, 22%, and 22.7% overhead at $R_{th}=0.7$, 0.8, and 0.9, respectively, while the BP decoding requires a 24.1% overhead. Thus, overhead is reduced as $R_{th}$ is decreased. On the contrary, the GE needs more symbol operations than the BP. Hence, the number of symbol operations is decreased as $R_{th}$ is increased, as shown in Table 3. Thus, the BP-GE decoding scheme requires 2.1% less overhead than the BP decoding at $R_{th}=0.8$ with the same number of symbol operations. However, the BP-GE decoding scheme with $R_{th}=0.7$ needs only 0.32 more symbol operations than the BP decoding scheme while 3% less overhead is required. Thus, overhead can be reduced by the BP-GE hybrid decoding while symbol operations are almost unchanged. Otherwise, the BP-GE hybrid decoding reduces much more overhead with a few more symbol operations.

V. Conclusion

Rateless coding has a special characteristic such that the code rate is determined at a receiver. Thus, it does not have to estimate and inform the erasure rate from the receiver to the transmitter. In addition, a rateless code can achieve a capacity-approaching characteristic if the overhead is minimized. However, the probability of recovering a new message is decreased by the uniform selection of messages. Hence, a new encoding scheme using nonuniform selection was proposed, and the performance was analyzed and compared with that of the conventional uniform encoding scheme. According to the results, the proposed scheme has less overhead and less computational complexity than the conventional scheme. Further, the BP-GE hybrid decoding scheme was also proposed to complement the drawbacks of the BP decoding scheme. The results show that the BP-GE hybrid decoding

---

**Table 1.** Average number of symbol operations according to encoding schemes ($k=500$).

<table>
<thead>
<tr>
<th>Encoding scheme</th>
<th>Symbol operations per message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uniform</td>
<td>10.7</td>
</tr>
<tr>
<td>$R_{th} = 0.1$</td>
<td>9.3</td>
</tr>
<tr>
<td>$R_{th} = 0.2$</td>
<td>9.46</td>
</tr>
<tr>
<td>$R_{th} = 0.3$</td>
<td>9.61</td>
</tr>
</tbody>
</table>

**Table 2.** Average number of symbol operations according to encoding schemes ($k=5,000$).

<table>
<thead>
<tr>
<th>Encoding scheme</th>
<th>Symbol operations per message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uniform</td>
<td>15.2</td>
</tr>
<tr>
<td>$R_{th} = 0.1$</td>
<td>14.1</td>
</tr>
<tr>
<td>$R_{th} = 0.2$</td>
<td>14.5</td>
</tr>
<tr>
<td>$R_{th} = 0.3$</td>
<td>14.7</td>
</tr>
</tbody>
</table>

**Table 3.** Average number of symbol operations according to decoding schemes ($k=500$).

<table>
<thead>
<tr>
<th>Decoding scheme</th>
<th>Symbol operations per message</th>
</tr>
</thead>
<tbody>
<tr>
<td>BP</td>
<td>9.3</td>
</tr>
<tr>
<td>$R_{th} = 0.7$</td>
<td>9.62</td>
</tr>
<tr>
<td>$R_{th} = 0.8$</td>
<td>9.36</td>
</tr>
<tr>
<td>$R_{th} = 0.9$</td>
<td>9.1</td>
</tr>
</tbody>
</table>
requires less overhead than the BP decoding while the computational complexity is almost unchanged. In addition, the overhead can be reduced further if a little more computational complexity is allowed.

References


Hyung Taek Lim
received his BS and MS in electronics engineering from Kyungpook National University, Daegu, Rep of Korea, in 2004 and 2006, respectively. He is currently working toward his PhD in electronics engineering at Kyungpook National University. His research interests include mobile broadcasting and error correcting code.

Eon Kyeong Joo
received his BS in electronics engineering from Seoul National University, Seoul, Rep. of Korea, in 1976 and his MS and PhD in electrical engineering from Ohio State University, Columbus, Ohio, USA, in 1984 and 1987, respectively. From 1976 to 1979, he was an officer of communication and electronics in the Republic of Korea Navy. From 1979 to 1982, he worked for the Korea Institute of Science and Technology (KIST), Seoul, Rep. of Korea, as a researcher. In 1987, he joined the faculty of the Department of Electronic Engineering, Kyungpook National University, Daegu, Rep. of Korea, where he is currently a professor in the School of Electronics Engineering. His research interests include digital communications, coding and decoding, modulation and demodulation, and signal processing for communications.